МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ВИПУСКНА РОБОТА

на тему:

"Комплексна система захисту інформації відділу менеджменту "

Завідувач випускаючої кафедри — **Довбиш А.С.**

Керівник роботи — **Проценко О.Б.**

Студент гр. КБ-61-8 — **Смаглюк М.П.**

СУМИ 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерних наук

Затверджую _____

Зав. кафедрою Довбиш А.С.

“_____” _____2020 р.

Завдання

до випускної роботи

Студента четвертого курсу, групи КБ-61-8 спеціальності “Кібербезпека” денної форми навчання Смаглюка Максима Петровича.

Тема: “**Комплексна система захисту інформації відділу менеджменту**”

Затверджена наказом по СумДУ

№_____ від _____2020 р.

Зміст пояснювальної записки: 1) Інформаційний огляд системи захисту інформації; 2) Вибір функціонального профілю захищеності оброблювальної інформації від несанкціонованого доступу; 3) Розробка і введення в дію КЗСІ ;

Дата видачі завдання “_____”_____2020 р.

Керівник випускної роботи _____ Проценко О.Б.

Завдання прийняв до виконання _____ Смаглюк М.П.

РЕФЕРАТ

Записка: 42 стор., 3 рис., 1 додаток, 15 джерел.

Об'єкт дослідження — Комплексна система захисту інформації

Мета роботи — розроблення комплексної системи захисту інформації є формування моделі загроз інформації та моделі порушника об’єкта інформаційної діяльності, розробка політики безпеки та системи документів з забезпечення захисту інформації в АС розрахунок та оцінка ризиків.

Результати — виконано комплекс робіт по розробці та впровадженню мір та заходів захисту підприємства. В проекті була розроблена комплексна система захисту інформації на підприємстві «Estmanagemen». При розробці були враховані особливості організації, такі як її невеликий розмір, але великий обсяг обробляємої інформації.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ЦІЛІСНІСТЬ ДОСТУПНІСТЬ, КОНФІДЕНЦІЙНІСТЬ, ЗАХИСТ, БЕЗПЕКА

ЗМІСТ

ВСТУП

Необхідність забезпечення захисту інформації а саме створення КСЗІ визначаються вимогами нормативно-правових документів або рішенням власника інформаційних ресурсів. Для характеристики основних властивостей інформації використовується модель СІА (конфіденційність, цілісність, доступність) але з урахуванням НД ТЗІ 2.5-004-99 критерії оцінки захищеності в комп'ютерних системах від несанкціонованого доступу з'являються й інші властивості (апелювання, підзвітність, достовірність, автентичність). Захист інформації в сучасних умовах стає більш складним за такими причинами як масове поширення засобів ЕОТ (електронної обчислювальної техніки), ускладнення шифрувальних технологій, необхідність захисту промислової, фінансової і комерційної таємниці, а не тільки державної та військової.

У даний час одержали широке поширення засоби і методи несанкціонованого отримання інформації. Сам процес створення полягає у здійсненні комплексу пов'язаних між собою заходів спрямованих на розроблення і впровадження інформаційної технології яка забезпечує оброку інформації в ІТС згідно з вимогами, встановленими нормативно- правовими актами та НД у сфері захисту інформації.

Побудова комплексної системи захисту інформації на підприємстві складний процес, багато в чому залежить від правильного розуміння діяльності організації. Даними для дослідження служить характеристики досліджуваного об'єкта. Технічним завданням на створення КСЗІ являєтеся організаційно технічний документ для виконання робіт щодо забезпечення захисту інформації в системі.

1 ІНФОРМАЦІЙНИЙ ОГЛЯД

1.1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА АВТОМАТИЗОВАНОЇ СИСТЕМИ УСТАНОВИ І УМОВ ЇЇ ФУНКЦІОНУВАННЯ

Компанія «Estmanagemen» займається управлінням чи допомогою в управлінні персоналом а також корегуванням дій на покращення роботи та її організації . Компанія веде підрахунки витрат та доходів при відкритті нових підприємств, крім цього компанія займається просуванням на ринок нових підприємств та приватних підприємців. Тому компанія займається аналізом ринку попиту на продукцію, що виробляється підприємствами і визначає основні тенденції виробництва у певний часовий період.

Загальна структурна схема та склад обчислювальної системи автоматизованої системи.

Обчислювальна система даної компанії є локальною мережею, яка складається з 8 комп'ютерів, що знаходяться в одному приміщенні Офіс знаходиться на першому поверсі будівлі. За генеральним планом у компанії 2 робочі кімнати. З яких 1 кімната – це робочій відділ компанії; кабінет головного директора компанії «Estmanagemen» та робочих місць працівників .

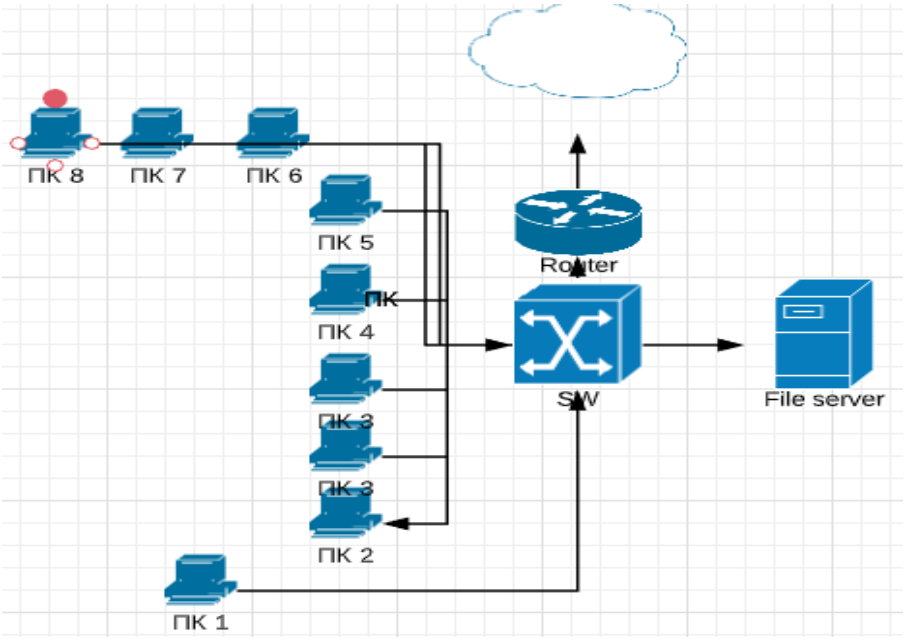

Рисунок 1 - Схема підключення комп'ютерів в мережу

Технічна характеристика обладнання

Таблиця 1.1

Комп’ютери, що використовуються для роботи персоналу: Dell Precision 7920 Tower (210-7920-6152)

Характеристика	Значення
Тип	Десктоп
Процесор	Intel Xeon Gold 6152
Частота, GHz	2,1
Оперативна пам’ять	DDR4-2666
Об’єм, GB	64
Стандарт	PC2-6400
Жорсткий диск	
Об’єм, GB	256
Інтерфейс	SATA
Графічний адаптер	
Чіпсет	NVIDIA Quadro P4000
Об’єм пам’яті, GB	8
Оснащення	
Вбудований оптичний накопичувач	DVD-RW
Звукова карта	Інтегрована
Зовнішні порти	4xUSB 3.1 Type-C, mini DisplayPort, HDMI, Thunderbolt 3, audio
Мережевий адаптер	1Gb Ethernet
Встановлена ОС	Windows 10

Таблиця 1.2

Комп’ютери, якими користуються директор компанії ARTLINE WorkStation W99 (W99v26)

Характеристика	Значення
Тип	Десктоп
Чіпсет	AMD x570
Процесор	
Тип процесора	AMD Ryzen 9 3950x
Частота, GHz	3,5

Оперативна пам’ять	
Об’єм, GB	128
Стандарт	DDR4-3200
Жорсткий диск	
Об’єм, GB	1000+500
Інтерфейс	SATA III, PCIe NVME m.2
Графічний адаптер	
Чіпсет	NVIDIA Quadro RTX 6000
Об’єм пам’яті, GB	24
Оснащення	
Вбудований оптичний накопичувач	DVD-RW
Звукова карта	Realtek ALC888S
Зовнішні порти	PS/2 keyboard/mouse combo port, 4xDisplayPort, HDMI port, 3xUSB 3.2 Gen 2, 1xUSB 3.2 Gen 2 (Type-C), 4xUSB 3.2 Gen 1, Optical S/PDIF out, , 2xUSB3.0)
Мережевий адаптер	10/100/1000
Встановлена ОС	Windows 10

Характеристика програмного забезпечення

Операційна система (ОС), з якою працюють користувачі, це Windows 10. Вибір цієї ОС оснований на тому, що дана версія Windows 10 спеціально розроблена для підприємств і має посилену політику безпеки і системи захисту.

Операційна система (ОС), що використовується на серверах компанії – Windows Server 2008 Standard Edition.

Для забезпечення захисту ПК від НСД і несанкціонованого використання ІзОД приводи оптичних накопичувачів відімкнені у всіх комп’ютерах у підприємстві, крім комп’ютера головного директора і адміністраторів безпеки.

Розмежування доступу до ПК створено за допомогою вбудованих засобів захисту в ОС Windows 10. Для кожного відділу створено свою робочу групу (домен) і користувачів, які можуть працювати лише у даній робочій групі, де вони мають наперед встановлені права. Користувача однієї робочої групи не може бути аутентифіковано у іншій.

При вході у систему на ПК завантажуються особисті дані з файлового сервера та сервера баз даних.

При побудові плану розташування робочих місць ми керувались наступними принципами:

- Екрани комп’ютерів не повинні бути повернуті до вікон або дверей;
- Робочі місця розміщені таким чином, щоб мінімізувати спостереження за роботою одних користувачів за іншими.

1.2 ПОСТАНОВКА ЗАДАЧІ

Метою розроби КСЗІ є впровадження заходів та засобів, які реалізують способи, методи, механізми захисту інформації від:

- витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;
- несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм, використання комп’ютерних антивірусів та ін.;
- спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Комплексна система захисту інформації надає загальну характеристика автоматизованої системи установи і умов її функціонування. Метою комплексної системи захисту інформації є формування моделі загроз інформації та моделі порушника об’єкта інформаційної діяльності, розробка політики безпеки та системи документів з забезпечення захисту інформації в АС розрахунок та оцінка ризиків.

Рисунок 2 - Ієрархічний підхід до забезпечення безпеки інформації

Комплексна система захисту інформації призначена для захисту інформації, що циркулює та зберігається у межах об’єкта інформаційної діяльності. КСЗІ створюється на основі Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», ДСТУ 3396.1-96, НД ТЗІ 1.1-002-99, НД ТЗІ 1.4-001-2000, НД ТЗІ 2.1-001-200, НД ТЗІ 3.7-001-99, НД ТЗІ 3.7-003-05.

2 ВИБІР ФУНКЦІОНАЛЬНОГО ПРОФІЛЮ ЗАХИЩЕНОСТІ ОБРОБЛЮВАНОЇ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.

Згідно з аналізом роботи ІТС та відповідних експертиз визначено, що на об’єкті циркулює інформація що потребує захисту. Ця інформація поділяється на відкриту інформацію, що потребує захисту та інформацію з обмеженим доступом. Інформація четвертої категорії (конфіденційна інформація) циркулює в АС класу «2».

Відповідно до ДСТУ 3396.1-96 визначається варіант захисту інформації. Для захищає мого об’єкта найбільш підходящим є такий варіант:

- досягнення необхідного рівня захисту ІзОД за допустимих затрат і заданого рівня обмежень видів ІД.

Відповідно до НД ТЗІ 2.5-005-99 потрібно визначити функціональний профіль захищеності інформації. Перш за все нам потрібно забезпечити конфіденційність інформації, яка визначена як ІзОД. Крім того у компанії обробляється відкрита інформація, що потребує захисту (деякі номери рахунків активів компанії, інформація про діяльність компанії і т. д.). Для такої інформації потрібно забезпечити цілісність.

Відповідно до НД ТЗІ 2.5-005-99 застосуємо функціональний профіль захищеності в КС, що входить до складу АС класу «2», з підвищеними вимогами до забезпечення конфіденційності і цілісності оброблюваної інформації.

Позначення послуг конфіденційності:

КД – довірча конфіденційність;

КА – адміністративна конфіденційність;

КО – повторне використання об’єктів.

КК – аналіз прихованих каналів

Позначення послуг цілісності:

ЦД – довірча цілісність;

ЦА – адміністративна цілісність;

ЦО – відкат.

Позначення послуг спостереженості:

НР – реєстрація;

НИ – ідентифікація і автентифікація;

НК – достовірний канал;

НО – розподіл обов’язків;

НЦ – цілісність КЗЗ;

НТ – самотестування при старті.

2.КЦ.5 – функціональний профіль номер три, що визначає вимоги до АС класу «2», призначених для обробки інформації, основною вимогою щодо захисту якої є забезпечення конфіденційності та цілісності інформації.

Розподіл обов'язків щодо виконання заходів, передбачених політикою безпеки

Адміністратор безпеки володіє всіма правами по установці і налаштуванню КСЗІ створює, видаляє облікові записи співробітників, слідкує за додержанням правил розмежування доступу, вносить зміни до них при зміні посади певного співробітника, а також при допуску до певної інформації.

Системний адміністратор слідкую за правильним функціонуванням комп’ютерної системи, проводить планові перевірки її компонентів, вирішує технічні проблеми АС при їх виникненні.

Працівник служби охорони проводить відео спостереження, реєструє відвідувачів у відповідному журна відповідає за дотриманням правил допуску до серверних приміщень та приміщень для зберігання документів, звітів про діяльність компанії, зареєстрованих носіїв інформації, даних відео нагляду та спостереження, журнали відвідувань і т. д., відповідає за безпеку установи і співробітників.

Дирекція координує роботу адміністратора безпеки та служби безпеки. Служба безпеки, системні адміністратори та адміністратори безпеки узгоджують свою роботу.

2.1 СИСТЕМА ДОКУМЕНТІВ З ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АС

Захист інформації в АС регламентується:

- Закон України “Про інформацію”;
- Закон України “Про захист інформації в автоматизованих системах”;
- Закон України “Про державну таємницю";
- Концепція технічного захисту інформації в Україні;
- ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення;
- ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт;
- ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення;
- НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу;
- НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;
- НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі;

- НД ТЗІ 2.1-001-01. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення;
- НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;
- НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;
- НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі;
- НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Нормативні, організаційно-розпорядчі та інші документи, що використовуються у АС:

- положення про захист інформації в АС;
- інструкції про порядок реалізації організаційних, первинних технічних та основних технічних заходів захисту, інструкції про порядок введення в експлуатацію КСЗІ, про порядок її модернізації, про порядок обробки ІзОД в АС, про порядок використання криптографічних засобів;
- правила управління паролями в АС, правила видачі, вилучення та обміну персональних ідентифікаторів, атрибутів розмежування доступу;
- інструкції, що встановлюють повноваження та відповідальність персоналу і користувачів;
- плани виконання робіт та здійснення окремих заходів з захисту інформації в АС.

В АС також складається календарний план робіт з реалізації заходів захисту інформації в АС, який містить такі розділи:

- організаційні заходи;
- контрольно-правові заходи;
- профілактичні заходи;

- інженерно-технічні заходи.

- робота з кадрами.

2.2 КРИТЕРІЇ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ СИСТЕМАХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

В контексті Критеріїв комп'ютерна система розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз.

Відповідно до НД ТЗІ 2.5-004-99 застосуємо критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу, приділяючи значну увагу забезпеченню конфіденційності і цілісності оброблюваної інформації:

КД-2. Базова довірча конфіденційність :

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта

КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта

КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес

КА-2. Базова адміністративна конфіденційність :

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження

КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом

керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта

КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту

КО-1. Повторне використання об'єктів

Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною

ЦД-1. Мінімальна довірча цілісність

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта

КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт

КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи

користувачів, які мають право ініціювати процес. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту

ЦА-2. Базова адміністративна цілісність

КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити. Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт. КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту

ЦО-1. Обмежений відкат

Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу

НР-2. Захищений журнал

Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються. КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки. Журнал реєстрації

повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події. КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації

НИ-2. Одиночна ідентифікація і автентифікація

Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ. Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування

НК-1. Однонаправлений достовірний канал

Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ. Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем

НО-2. Розподіл обов'язків адміністраторів

Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі. Користувач повинен мати

можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі

НЦ-2. КЗЗ з гарантованою цілісністю

Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів. КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування. Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ

НТ-2. Самотестування при старті. Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження

3 РОЗРОБКА І ВВЕДЕННЯ В ДІЮ КЗСІ

3.1 РОЗРОБКА ПОЛІТИКИ БЕЗПЕКИ

Цілі реалізації політики безпеки

Основною ціллю реалізації політики безпеки є забезпечення ефективного функціонування компанії, для чого необхідно забезпечити захист оброблюваної на підприємстві інформації від несанкціонованого доступу. Політика безпеки має на меті розробку та впровадження правил та норм внутрішнього режиму праці на підприємстві, режиму доступу та допуску до важливих об’єктів, їх охорона, середовище розміщення

Рисунок 3. Основні правила забезпечення політики безпеки інформації

Загальні вимоги політики безпеки

Під час розробки політики безпеки були враховані технологія обробки інформації, описані вище моделі порушників і загроз, особливості ОС, фізичного середовища та інші чинники. В АС реалізовано декілька різних політик безпеки, які істотно відрізняються. Як складові частини загальної політики безпеки в АС існують політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації.

Політика безпеки стосується: інформації (рівня критичності ресурсів АС), взаємодії об’єктів (правил, відповідальності за захист інформації, гарантій захисту), області застосування (яких складових компонентів АС політика безпеки стосується, а яких – ні).

Політика безпеки розроблена таким чином, що вона не потребує частої модифікації. Політика безпеки передбачає використання всіх можливих

заходів захисту інформації(правові та морально-етичні норми, організаційні, фізичні, технічні заходи) і визначає правила та порядок застосування в АС кожного з цих видів.

Політика безпеки базується на наступних основних принципах:

- системності;
- комплексності;
- неперервності захисту;
- достатності механізмів і заходів захисту та їхньої адекватності загрозам;
- гнучкості керування системою захисту, простоти і зручності її використання;
- відкритості алгоритмів і механізмів захисту, якщо інше не передбачено окремо.

Політика безпеки дає гарантії того, що:

- в АС забезпечується адекватність рівня захисту інформації рівню її критичності;
- реалізація заходів захисту інформації є рентабельною;
- в будь-якому середовищі функціонування АС забезпечується оцінюваність і перевіряємість захищеності інформації;
- забезпечується персоніфікація положень політики безпеки (стосовно суб'єктів АС), звітність (реєстрація, аудит) для всіх критичних з точки зору безпеки ресурсів, до яких здійснюється доступ в процесі функціонування АС;
- персонал і користувачі забезпечені достатньо повним комплектом документації стосовно порядку забезпечення захисту інформації;
- всі критичні з точки зору безпеки інформації технології (функції) АС мають відповідні плани забезпечення неперервної роботи та її поновлення у разі виникнення непередбачених ситуацій;

- враховані вимоги всіх документів, які регламентують порядок захисту інформації в АС , та забезпечується їхнє суворе дотримання.

3.2 ФОРМУВАННЯ МОДЕЛІ ПОРУШНИКА ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Під порушником розуміється особа, яка зробила спробу виконання заборонених операцій помилково, не знаючи або навмисно зі злим помислом (корисним інтересом) або без таких (заради гри, самоствердження), заради самоствердження або помсти, використовуючи для цього різні способи і методи, можливості і засоби.

Порушник може використовувати різноманітні методи та засоби для доступу до ІзОД. Якщо порушник діє навмисне, з корисних мотивів, то будемо називати його зловмисником. Зловмисники винятково якісно вивчають системи безпеки в ІТС перед проникненням до неї.

Необхідно оцінити збитки, які можуть мати місце у випадку витоку інформації або при будь-якому іншому порушенні системи безпеки, а також ймовірність нанесення подібних збитків. Для визначення адекватності вартості системи захисту, слід зіставити розміри збитків і ймовірність їх нанесення з розмірами затрат на забезпечення захисту. Проте, реальну вартість інформації оцінити дуже важко, тому зазвичай використовують не кількісні, а якісні експертні оцінки. Найчастіше будується неформалізована модель порушника (зловмисника), що відображає причини й мотиви дій, його можливості, знання, цілі, основні шляхи досягнення поставлених цілей – способи реалізації загроз, місце і характер дії, можлива тактика і т. д. Для досягнення поставлених цілей зловмисник повинен прикласти деякі зусилля і затратити деякі ресурси.

Порушником по відношенню до АС можуть бути особи з персоналу і користувачів системи; сторонні особи.

Можливі внутрішні порушники :

- кінцеві користувачі (оператори системи); персонал;(перший рівень)

- особи, що обслуговують технічних засобів (третій рівень);
- співробітники відділу розробки і супроводження програмного забезпечення (четвертий рівень);
- співробітники служби безпеки АС (перший рівень);
- керівники різних рівнів (перший рівень).

Можливі зовнішні порушники (сторонні особи):

- технічний персонал, обслуговуючий будівлю (перший рівень);
- клієнти (перший рівень);
- представники організацій-конкурентів (другий рівень);
- відвідувачі запрошені з будь-якого приводу (другий рівень).

Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами КС. Виділяються чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

- **перший рівень** визначає найнижчий рівень можливостей проведення діалогу з КС – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
- **другий рівень** визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;
- **третій рівень** визначається можливістю управління функціонуванням КС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;
- **четвертий рівень** визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів КС, аж до включення до складу КС власних засобів з новими функціями обробки інформації.

Припускається, що в своєму рівні порушник – це фахівець вищої кваліфікації, який має повну інформацію про КС і КЗЗ.

Порушник може здійснювати несанкціонований доступ до інформації або під

час роботи автоматизованої системи, або в період неактивності автоматизованої системи, або ж суміщаючи робочий і не робочий час.

У КСЗІ на виділеному об’єкті передбачаються, розглядаються і розробляються усі чотири рівні порушників.

Таблиця 3

Модель порушника

№	Користувач АС	Рівень порушника
1.	Внутрішні	
1.1	Директор	III
1.2	Системний Адміністратор	IV
1.3	Персонал	II
2.	Зовнішні	
2.1	Працівник служби охорони	III
2.2	Працівник комунальних служб	III
2.3	Конкуренти	II
2.3	Клієнт	II

3.3 ФОРМУВАННЯ МОДЕЛІ ЗАГРОЗ ІНФОРМАЦІЇ ОБ’ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Основою для проведення аналізу ризиків і формування вимог до КСЗІ є розробка моделі загроз для інформації та моделі порушника.

Для створення моделі загроз необхідно скласти перелік суттєвих загроз, описати методи і способи їхнього здійснення.

Необхідно визначити, якими з можливих способів можуть здійснюватися загрози в АС:

- технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;

- каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;
- несанкціонованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів.

Загрози для інформації, що обробляється в АС, залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно АС і повинні враховуватись у моделі загроз, наприклад:

- зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);
- збоїв і відмови у роботі обладнання та технічних засобів АС;
- наслідки помилок під час проектування та розробки компонентів АС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);
- помилки персоналу (користувачів) АС під час експлуатації;
- навмисні дії (спроби) потенційних порушників.

Необхідно визначити перелік можливих загроз і класифікувати їх за результатом впливу на інформацію, тобто на порушення яких властивостей вони спрямовані (конфіденційності, цілісності та доступності інформації), а також порушення спостережності та керованості АС.

Випадковими загрозами суб’єктивної природи (дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

- дії, що призводять до відмови АС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв’язку, видалення даних, програм та ін.);
- ненавмисне пошкодження носіїв інформації;
- неправомірна зміна режимів роботи АС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);
- неумисне зараження ПЗ комп’ютерними вірусами;
- невиконання вимог до організаційних заходів захисту чинних в АС розпорядчих документів;
- помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;
- будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;
- неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення та ін.);
- наслідки некомпетентного застосування засобів захисту;
- інші. Навмисними загрозами суб’єктивної природи, спрямованими на дезорганізацію роботи АС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути:
- порушення фізичної цілісності АС (окремих компонентів, пристроїв, обладнання, носіїв інформації);
- порушення режимів функціонування (виведення з ладу) систем життєзабезпечення АС (електроживлення, заземлення, охоронної сигналізації, вентиляції та ін.);

- порушення режимів функціонування АС (обладнання і ПЗ);
- впровадження і використання комп’ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;
- використання засобів перехоплення побічних електромагнітних випромінювань і наводів, акусто-електричних перетворень інформаційних сигналів;
- використання (шантаж, підкуп тощо) з корисливою метою персоналу АС;
- крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);
- несанкціоноване копіювання носіїв інформації;
- читання залишкової інформації з оперативної пам’яті ЕОМ, зовнішніх накопичувачів;
- одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача (“маскарад”);
- неправомірне підключення до каналів зв’язку, перехоплення даних, що передаються, аналіз трафіку тощо;
- впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);
- інші.

Таблиця 3.1

Класифікація потенційних загроз інформації, що обробляється в АС

№	Джерело	Природа		Загроза	Наслідки порушення				Ресурси
					К	Ц	Д	С	
1	Зовнішні	Об’єктивна		Стихійні явища		+	+		Всі
2	Зовнішні	Об’єктивна		Збої та відмови системи електроживлення		+	+		Всі
3	Внутрішні	Об’єктивна		Збої та відмови обчислювальної техніки		+	+		Всі
4	Внутрішня	Об’єктивна		Збої, відмови та пошкодження носіїв інформації		+	+		Всі
5	Внутрішня	Об’єктивна		Збої та відмови програмного забезпечення		+	+		Всі
6	Внутрішня	Об’єктивна		Відмова в доступі користувачу АС в результаті помилки ПЗ			+		{ІК_КЗЗ}, {ІЗК}
7	Зовнішня	Суб’єктивна	Навмисна/ ненавмисна	Ураження програмного забезпечення комп’ютерними вірусами	+	+	+	+	всі
8	Внутрішня	Суб’єктивна	Навмисна/ ненавмисна	Несанкціоноване внесення змін до технічних засобів, в програмне забезпечення, що призводять до зміни режиму роботи чи відмови АС		+	+	+	{ЗАЗ_КЗЗ}, {СПЗ_КЗЗ}, {ТІ_КЗЗ}
9	Внутрішня	Суб’єктивна	Навмисна/ ненавмисна	Порушення адміністратором безпеки реалізації ПРД	+	+	+	+	{ТІ_КЗЗ},{І_ЖР}, {ІК}, {ІЗК}
10	Внутрішня	Суб’єктивна	Ненавмисна	Втрата атрибутів розмежування доступу	+	+	+		всі
11	Внутрішня	Суб’єктивна	Навмисна	Неправомірне впровадження і використання забороненого політикою безпеки ПЗ	+	+	+	+	всі
12	Зовнішня	Суб’єктивна	Навмисна	Використання з корисливою метою персоналу АС	+	+	+	+	{ІК}, {ІЗК}
13	Зовнішня	Суб’єктивна	Навмисна	Несанкціонований доступ до приміщення АС	+	+	+	+	всі
14	Зовнішня	Суб’єктивна	Навмисна	Вербування працівників підприємства	+	+			всі
15	Зовн./ Внутр.	Суб’єктивна	Навмисна	Розкрадання матеріальних носіїв інформації	+	+			всі
16	Внутрішня	Суб’єктивна	Навмисна	Читання залишеної інформації	+				{ІК}, {ІЗК}
17	Внутрішня	Суб’єктивна	Ненавмисна	Ненавмисне псування матеріальних носіїв інформації			+		всі

3.4 КЛАС АВТОМАТИЗОВАНОЇ СИСТЕМИ

Згідно з НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні класи захищеності оброблюваної інформації від несанкціонованого доступу» в фінансово-консалтинговій компанії інформація циркулює та обробляється в АС класу «2» [6]

АС класу «2», це – локалізований багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності.

2.КЦ.5 = { КД-3, КА-3, КО-1, КК-1,

ЦД-1, ЦА-3, ЦО-2,

НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2 }

В складі АС функціонують такі засоби захисту:

- сенсори розбитого скла;
- відеоспостереження;
- пожежна сигналізація;
- охоронна система;
- джерела безперебійного живлення;
- металеві решітки;
- кабельне обладнання.

Характеристики фізичного середовища

Під час аналізу фізичного середовища потрібно також знайти та локалізувати можливі канали витоку інформації, що виходять за межу контрольованої зони.

Це такі канали як:

- канали витоку інформації по ланцюгам електроживлення;
- канали витоку інформації по ланцюгам заземлення;
- канали витоку інформації по вентиляційним системам.

Територія компанії охороняється штатом охоронців у кількості 4 осіб. Крім того ведеться відео нагляд за територією, та в середині приміщення.

У компанії запроваджена система електронних пропусків, що зменшує

імовірність загроз вчинити викрадення інформації зловмисником, що не є робітником фірми, не опосередковано з її території.

Технічні характеристики каналів зв'язку

Для побудови локальної мережі використовується екранована вита пара. Згідно зі стандартами, для ізоляції мережевого кабелю, використовуємо екрановані металеві короба. Завдяки цьому буде значно зменшена імовірність загроз з боку витоку інформації технічними каналами зв'язку.

Характеристики інформації, що обробляється

Інформація, що обробляється в АС є власністю даної фірми та її клієнтів. В АС даного підприємстві обробляється відкрита та конфіденційна інформація. До конфіденційної інформації відносяться дані, що пов'язані з клієнтами фірми та їх справами, технологічна та ключова інформація. Інформація загального користування є відкритою інформацією.

Таблиця 5

№	Шифр	Назва	Тип доступу
1	{БД.К}	База даних – клієнтів	конфіденційна
2	{Д}	Договори	відкрита
3	{П.О}	Перелік обладнання	відкрита
4	{БД.П}	База даних – працівників	Конфіденційна
5	{БД.З.Р}	База даних засобів і ресурсів	конфіденційна
6	{БД.Т.К}	База даних телефонів клієнтів	конфіденційна
7	{БД.Т.П}	База даних телефонів працівників	відкрита
8	{П}	Партнери	відкрита
9	{Ж.К.}	Журнал користувачів	відкрита
10	{Ж.Д.}	Журнал досягнень	відкрита

Характеристики персоналу та користувачів автоматизованої системи

До середовища персоналу установи та користувачів автоматизованої системи належать технічний та обслуговуючий персонал, системні адміністратори, адміністратор безпеки, працівники служби охорони, бухгалтери, маркетологи, секретар, працівники відділу роботи з клієнтами, керівники відділів, директор.

Найнижчі повноважень щодо допуску до відомостей, які обробляються в ІТС мають технічний та обслуговуючий персонал, а також працівники служби охорони. Достатньо високі повноваження мають працівники маркетингового відділу та відділу інформаційних технологій, дирекція. Найбільше повноваження щодо управління КСЗІ має адміністратор безпеки, дещо нижчий пріоритет у працівників служби безпеки та системних адміністраторів. Вхід до серверних приміщень та приміщень для зберігання документів, звітів про діяльність компанії, зареєстрованих носіїв інформації, даних відео нагляду та спостереження, журнали відвідувань і т. д. мають лише дирекція та особи, яким надається допуск до цих матеріалів.

ВИСНОВОК

В кваліфікаційній роботі бакалавра була розроблена комплексна система захисту інформації на підприємстві «Estmanagemen». При розробці були враховані особливості організації, такі як її невеликий розмір, але великий обсяг обробляємої інформації. По результату роботи можливо зробити висновки про ефективність розробленої системи по декільком критеріям:

- загальний річний збиток, розрахований методом еквівалентної шкоди, набагато вищій від запропонованої ціни захисту її обслуговування в річному періоді;
- величина сумарного річного збитку неприємлива для організації, тим самим ведення КЗСІ є невідкладною мірою для стабільної діяльності підприємства;
- витрати на ведення в експлуатацію зіставляють лише десяту частину чистого заробітку компанії що вважається приємливим.

По результату роботи с урахуванням висновків про ефективність системи, можна рекомендувати КЗСІ на впровадження у роботу компанії с допоміжним та приватними доопрацюванням.

СПИСОК ЛІТЕРАТУРИ

1. П О С Т А Н О В А Про затвердження Положення про кіберзахист та інформаційну безпеку в платіжних системах та системах розрахунків - https://bank.gov.ua/doccatalog/document?id=78399302
2. Про внесення змін до Закону України "Про інформацію" №2938-VI від 13.01.2011. – Відомості Верховної Ради України 2011, №32, ст. 313. – (Серія видань "Законодавство України").
3. Закон України "Про захист персональних даних" №2297-VI від 01.06.2010. – Відомості Верховної Ради України 2010, № 34, ст. 481. – (Серія видань "Законодавство України").
4. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. В 2-х томах. – К.: Арий, 2008. – Том II.
5. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22 від 28.04.99. – (Серія видань "Нормативний документ").
6. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України №22 від 28.04.1999. – (Серія видань "Нормативний документ").
7. Про внесення змін до Закону України "Про захист інформації в автоматизованих системах" №2594-IV від 31.05.2005. – Відомості Верховної Ради України 2005, №26, ст. 347. – (Серія видань "Законодавство України").
8. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. – Затверджено наказом ДСТСЗІ СБ України №125 від 8.11.2005. – (Серія видань «Нормативний документ»).

9. Положення про Державну експертизу в сфері технічного захисту інформації. – Затверджено наказом Адміністрації ДССЗЗІ України №93 від 16.05.07. – Офіційний вісник України. – 2007. – №52, ст. 2153. – (Серія видань «Нормативний документ»).
10. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. – Затверджено наказом Адміністрації ДССЗЗІ України №65 від 12 березня 2011. – (Серія видань «Нормативний документ»).
11. НД ТЗІ 1.1-005-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення. – Затверджено наказом Адміністрації ДССЗЗІ України №232 від 12.12.2007.- (Серія видань «Нормативний документ»).
12. НД ТЗІ 3.1-001-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи. – Затверджено наказом Адміністрації ДССЗЗІ України №232 від 12.12.2007. – (Серія видань «Нормативний документ»).
13. НД ТЗІ 3.3-001-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації. – Затверджено наказом Адміністрації ДССЗЗІ України №232 від 12.12.2007. – (Серія видань «Нормативний документ»).
14. НД ТЗІ 2.1-002-07. Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення. – Затверджено наказом Адміністрації ДССЗЗІ України №232 від 12.12.2007. – (Серія видань «Нормативний документ»). НД ТЗІ 1.6-003-04. Створення комплексів технічного захисту інформації на о’єктах інформаційної діяльності.

ДОДАТОК

Інструкції користувача та адміністратора АС

Посадова інструкція адміністратора автоматизованої системи управління компанії «Estmanagemen»

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Ця посадова інструкція визначає статус, функціональні обов'язки, права і відповідальність адміністратора системи управління компанії «Estmanagemen» Адміністратор системи призначається на посаду та звільняється з посади розпорядженням директора або власника компанії.

.

КВАЛІФІКАЦІЙНІ ВИМОГИ

- Повна вища освіта відповідного професійного спрямування за освітньо-кваліфікаційним рівнем магістра, спеціаліста.
- Стаж роботи за фахом не менше 3 років.

ЗАВДАННЯ, ОБОВ'ЯЗКИ ТА ПОВНОВАЖЕННЯ

Адміністратор системи:

1) Повинен розробити/доопрацювати внутрішні документи щодо інформаційної безпеки та кіберзахисту у сфері переказу коштів (далі – документи з кіберзахисту) з урахуванням вимог цього Положення та затвердити їх керівником, його заступником або керівним органом суб'єкта платіжного ринку (далі – керівництво);

2) підтримувати документи з інформаційної безпеки та кіберзахисту в актуальному стані та здійснювати їх перегляд не рідше одного разу на рік;

3) розмістити сервери, що використовуються для приймання, оброблення, передавання електронних документів на переказ, збереження архівів, та мережеве обладнання, що забезпечує захист їх внутрішньої мережі, у серверних приміщеннях на території України;

4) визначити та запровадити посилені вимоги до парольної політики для привілейованих облікових записів (довжина та складність паролів, частота зміни) та/або застосовувати багатофакторну автентифікацію для таких облікових записів;

5) забезпечити дотримання вимог до логінів та паролів;

6) вжити заходів щодо обмеження використання програмного забезпечення (далі – ПЗ) та технічних пристроїв, розробником яких є юридична чи фізична особа-резидент держави-агресора;

7) забезпечити контроль за цілісністю клієнтського ПЗ, що реалізоване у вигляді програмного модуля, шляхом перевірки значень хеш-функцій на нього;

8) зберігати захищеними від несанкціонованого доступу облікові дані та паролі доступу до серверного і мережевого обладнання ключових суб'єктів платіжного ринку;

9) інформувати відвідувачів свого веб-сайта про перехід за зовнішнім посиланням у разі необхідності в переправленні (редиректі) на інший веб-сайт.

10) співпрацює з працівниками інших структурних підрозділів виконкому, представниками установ, організацій щодо вирішення питань, пов'язаних із його службовою діяльністю;

11) бере участь в аналізі та ліквідації аварійних, екстремальних та непередбачених ситуацій, пов'язаних з роботою інформаційно-телекомунікаційної системи;

12) бере участь в адмініструванні інформаційно-аналітичних баз даних;

13) відповідальний за збереження інформації, резервне копіювання та архівацію даних в інформаційних системах;

14) виконує обов'язки адміністратора ресурсів, адміністратора серверів, адміністратора систем антивірусного захисту інформації, адміністратора локальної обчислювальної мережі, адміністратора системи електронного документообігу ASKOD;

15) впроваджує та супроводжує загальносистемні програмні засоби;

16) проводить тестування і ремонт окремих пристроїв, засобів обчислювальної техніки, кабельних ліній локальної мережі;

17) забезпечує технічний супровід вживаних локальних мереж і програмного забезпечення;

18) вивчає існуюче програмне забезпечення, новітні розробки (операційні системи, системи управління базами даних, телекомунікаційні комплекси, засоби захисту та збереження інформації тощо) та надає пропозиції відносно доцільності їх застосування;

19) бере участь в розслідуванні випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження заводу даних таких подій, вжиття заходів у разі виявлення спроб несанкціонованого доступу до ресурсів автоматизованих систем, порушення правил експлуатації засобів захисту інформації або інших дестабілізуючих факторів;

МАЄ ПРАВО

Адміністратор системи має право:

1) користуватися правами і свободами;

2) на соціальний і правовий захист відповідно до свого статусу;

3) представляти за дорученням керівництва інтереси відділу в інших управлінських структурах з питань, що входять до його компетенції;

4) використовувати відповідну статистичну інформацію, інші дані від державних органів виконавчої влади, їх посадових осіб підприємств, установ, організацій, громадських об’єднань необхідні для виконання посадових обов’язків;

5) вступати у взаємостосунки з підрозділами сторонніх установ і організацій для вирішення оперативних питань службової діяльності, що входять у функціональні обов’язки;

6) вносити на розгляд керівництва пропозиції щодо вдосконалення

роботи відділу.

ВІДПОВІДАЛЬНІСТЬ

Адміністратор системи несе відповідальність за:

1) бездіяльність або неналежне виконання посадових обов'язків;

2) неналежне виконання чинного законодавства; за вчинення корупційних правопорушень винні особи притягаються до кримінальної, адміністративної, цивільно-правової та дисциплінарної відповідальності;

3) неналежне дотримання норм етики посадової особи;

4) обробку, збереження та захист персональних даних та конфіденційної інформації, відповідно до Закону України „Про захист персональних даних".

УМОВИ РОБОТИ

Режим роботи Адміністратора системи встановлюється відповідно до Правил внутрішнього трудового розпорядку та колективного договору.

У зв'язку з виробничою необхідністю Адміністратор системи може відбувати у службові відрядження (зокрема місцевого значення).

З інструкцією

ознайомлений _____ _____

Посадова інструкція користувача автоматизованої системи управління компанії «Estmanagemen»

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Інструкція визначає організаційно-правові основи щодо забезпечення безпеки експлуатації програмного комплексу захисту захищеного з'єднання.

Ця Інструкція розроблена у відповідності до вимог законодавчих актів та нормативних документів, які регламентують захист конфіденційної інформації або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також нормативних документів з технічного захисту інформації.

Вимоги цієї Інструкції повинні виконуватися в усіх режимах функціонування автоматизованої системи (далі - АС) управління.

Користувач у своїй роботі керується цією Інструкцією, Політикою інформаційної безпеки навчального закладу, керівними і нормативними документами України в галузі технічного захисту інформації, експлуатаційною документацією на встановлені на об'єкті інформатизації системи захисту від несанкціонованого доступу до інформації.

Користувач несе персональну відповідальність за свої дії.

Методичне керівництво роботою Користувача здійснюється особою, яка визначена відповідальною за внесення відомостей та даних від управління компанії «Estmanagemen», яка призначена наказом керівника управління для роботи в клієнтському веб-сервісі.

ПРАВА ТА ОБОВ'ЯЗКИ

1.1 Права Користувача:

2.1.1. Запитувати та одержувати від Адміністратора всю необхідну для виконання службових обов'язків інформацію.

2.1.2. Вимагати від Адміністратора своєчасного повідомлення про готовність технічних і програмних засобів робочої станції до експлуатації.

2.1.3. Звертатися до Адміністратора за консультаціями з питань забезпечення інформаційної безпеки технологічних процесів обробки інформації на закріплених за ним засобах.

2.1.4. Подавати обґрунтовані пропозиції Адміністратору про припинення інформаційного обміну або зміну режиму функціонування комплексу;

2.1.5. Ініціювати та брати учать у службових розслідуваннях за фактами порушення встановлених вимог забезпечення інформаційної безпеки, несанкціонованого доступу, втрати, пошкодження інформації, що захищається, та ввірених йому технічних засобів РС.

2.1.6. Користуватися наданим йому програмним забезпеченням клієнтського місця РС.

2.1.7. Звертатися до Адміністратора у разі несправності програмного забезпечення клієнтського місця РС.

2.1.8. Вимагати від Адміністратора скасування, блокування або поновлення своїх атрибутів авторизації.

1.2 Користувач зобов’язаний:

1.2.1 Знати і виконувати вимоги чинних нормативних та керівних документів, а також внутрішніх інструкцій, керівництва по захисту інформації і розпоряджень, що регламентують порядок дій із захисту інформації.

1.2.2 Ознайомитись та дотримуватись вимог документів, що визначають порядок підключення РС Користувача до клієнтських веб-сервісів.

1.2.3 Виконувати на РС тільки ті процедури, які визначені йому для роботи в клієнтському веб-сервісі.

1.2.4 Знати і дотримуватися встановлених вимог, по режиму обробки обліку, зберігання та пересилання носіїв інформації, забезпечення безпеки ПД, а також керівних та організаційно-розпорядчих документів.

1.2.5 Дотримуватися вимоги парольної політики.

1.2.6 Дотримуватися правил при роботі в мережах загального доступу або міжнародного обміну - Інтернет і інших.

1.2.7 Негайно повідомляти Адміністратору комплексу про незвичні параметри TCP-пакетів, що проходить через захищене з'єднання (велика кількість напіввідкритих з'єднань тощо).

1.2.8 Зберігати в таємниці особистий ключ та приймати всі можливі заходи для запобігання його втраті, розкриттю, перекручуванню та несанкціонованому використанню.

1.2.9 Використовувати особистий ключ виключно для здійснення захищеного з'єднання з клієнтським веб-сервісом, та додержуватися інших обмежень щодо використання атрибутів авторизації.

1.3 Користувачу забороняється:

- розголошувати інформацію, що захищається третім особам;

- використовувати особистий ключ у разі його компрометації або якщо він заблокований;

- копіювати інформацію, що захищається на зовнішні носії;

- відключати (блокувати) засоби захисту інформації;

- повідомляти (або передавати) стороннім особам особисті ключі та атрибути доступу до ресурсів клієнтського веб-сервісу;

- навмисно використовувати недокументовані властивості і помилки в програмному забезпеченні або в налаштуваннях засобів захисту, які можуть привести до виникнення кризової ситуації.

ОРГАНІЗАЦІЯ ПАРОЛЬНОГО ЗАХИСТУ

Особисті паролі доступу до елементів веб-сервісу видаються користувачам Адміністратором АС управління.

Дотримування визначених правил формування пароля. Під час введення паролів необхідно виключити можливість його підглядання сторонніми особами або технічними засобами (відеокамери та ін.). Правила зберігання пароля:

- забороняється записувати паролі на папері, у файлі, електронної записнику та інших носіях інформації, в тому числі на предметах; забороняється повідомляти іншим користувачам особистий пароль і реєструвати їх в системі під своїм паролем. Своєчасно повідомляти Адміністратору інформаційної безпеки про втрату, компрометації, несанкціонованому зміну паролів і несанкціонованому зміну термінів дії паролів.

ВІДПОВІДАЛЬНІСТЬ

Користувач несе відповідальність за дотримання вимог цієї Інструкції, а також інших нормативних документів в галузі захисту інформації. За розголошення інформації обмеженого доступу, а також за порушення порядку роботи з документами або машинними носіями, що містять таку інформацію, працівники можуть бути притягнуті до дисциплінарної або іншої, передбаченої законодавством відповідальності.

За розголошення інформації обмеженого доступу, порушення порядку роботи з документами або машинними носіями, що містять таку інформацію, працівники можуть бути притягнуті до дисциплінарної або іншої, передбаченої законодавством відповідальності.